Transactions of the VŠB - Technical university of Ostrava Vol. VII, No. 1, 2012
Safety Engineering Series p. 53 - 58

PROTECTION OF PUBLIC UNIVERSITIES PREMISES VIA AN IMPLEMENTATION OF RADIO FREQUENCY IDENTIFICATION OF PEOPLE

Martin KONEČNÝ[1], Ondřej STONIŠ[2], Radomír ŠČUREK[3]

Review article

Abstract: The article is focused on the characteristics of the public university building (hereinafter the PU) in terms of its physical protection, security risks identification and application of Radio Frequency Identification technology (hereinafter the RFID), as a potential efficient solution in increasing the level of security in the organization. The RFID technology presents an innovative element of contact-free identification and localization of persons with a specific system structure, which includes defining a principle of operation of primary components, such as the transponder and the reader. The scope of RFID usability is diverse. However, the article deals with the potential implementation of these systems within the PU premises and as the technical device, focused on significant contribution to risk management and protection of individuals, property or other assets of particular organization.

Key words: Physical protection, public universities, RFID, transponder, reader.

Introduction

Safety considerations and the resulting practical measures and actions are part of human history from the very beginning of civilization. These considerations have always corresponded to the achieved technology and material level. If we focus on the security, we can say that it is a state of the system, where the probability of harm to protected interests is accepted. From the beginning of 21st century the Czech Republic (CR) faces new security risks, the range of which is going to graduate further. The representatives of this group of risks include terrorism, organized crime and potential use of weapons of mass destruction. These threats and their possible elimination, but first of all prevention in this field, necessitates in a specific consistently coordinated support of the research as the integral part of the Czech security system. Closely to this relates the typology of security risks and threats as defined by the Security Policy Department of the Ministry of the Interior for 2010 (Řehák and Giertlová, 2011).

In the area of prevention, we must attach a lot of importance especially to buildings or institutions that make contacts or cooperate with countries that are the primary targets of terrorist attacks (e.g. USA, Great Britain). This category of buildings can include public universities as they cooperate with a number of similar institutions located in these countries and provide student exchanges, cooperate on significant science and research projects, etc., which might be a potential cause of terrorist attack. An important fact is that tens or hundreds of people, primarily students, employees and other public move in PU buildings throughout the day. These institutions are often visited by prominent politicians and statesmen on the occasion of various lectures, conferences or ceremonial events. These people undoubtedly represent potential targets of terrorist attack and therefore a threat for the PU building itself, including people occurring within. However, the buildings of public universities are not exposed only to external attacks. Serious threats to security are also a violence and aggression among students or teachers, which is often problematic to determine than from the standard offender. Variety of preventive programs against violence at school, which are primarily aimed at students, is being created. The reason is that the violence has reached an unacceptable level

[1] VŠB - Technical University of Ostrava, Faculty of Safety Engineering, Department of Security Service, Ostrava, Czech Republic, martin.konecny.st2@vsb.cz

[2] VŠB - Technical University of Ostrava, Faculty of Safety Engineering, Department of Security Service, Ostrava, Czech Republic, ondrej. stonis@vsb.cz

[3] VŠB - Technical University of Ostrava, Faculty of Safety Engineering, Department of Security Service, Ostrava, Czech Republic, radomir.scurek@vsb.cz

and thefts, assaults and homicides by students are no exceptions worldwide. Today students can easily get hold of a gun or a stubbing weapon. It remains a matter of time before incidents from abroad become a reality in the CR as well. This consideration is confirmed by the recent incident of knife attack on the primary school in Havířov, where a teacher was hurt. The attack was caused by a number of cutting and stabbing wounds. Due to the concentration of people moving in public universities and existing organization measures, similar attacks cannot be precluded and organizations have to take all possible preventive measures.

For this reason, it is therefore necessary to establish certain procedures and methods within the prevention, including the application of effective technology, enabling to eliminate identified risks and threats.

The risk management is an important preventive and effective element in the physical protection of public universities but still provided the appropriate choice of strategy and defining effective security measures designed to optimize the risks and losses arising from adverse situations and phenomena. However, despite all the prevention dedicated to the Risk Management, the organization cannot exclude a number of negative phenomena, which can lead to safety hazard to people and other assets. Those are emergency situations that are artificially induced and can be characterized as accidental, unexpected, socially dangerous, with a considerable negative impact on human health, property and the environment. This category of incidents can include placement of the booby-trap system, burglary, theft and other illegal activities. Perpetrators of these crimes can be divided into external attackers (terrorists, criminal offenders), internal attackers (employees and students) or a combination of both types of offenders, which is very efficient in terms of leading the attack. With a large number of people moving within the PU buildings, it is currently impossible to competently identify who and for what purpose had visited the facility. Public universities are with its vulnerability opened to all visitors and thus represent an easy target of terrorist attack and other forms of crime. Due to the insufficient level of security and protection of persons, property and other assets of the organization, located on the premises of public universities, the risk of vulnerability and threats is significant and we must pay attention to it (Ščurek and Konečný, 2011).

Materials and methods

Characteristics of selected issue

The following part of the article will define a direction of security research, resulting from current threats and risks within the public universities. We can say that it is a multidisciplinary trend which enables an application of a number of disciplines. Given the character of PU buildings, the list includes particularly the segment of security, dealing with threats to protected interests, which is the potential attack occurrence rate (terrorist, extremist, criminal, etc.) in the location in question and is determined by the ability and intention of the perpetrators and by the vulnerability of protected interests of the state.

The degree of protection of persons and property determines a safety policy of each organization presented by safety management, which individually defines the level and strategy of standard protection with mechanical, electrical and electronic elements and arrangements with the protection regime and physical protection, complemented with insurance. Increasing the level of safety is achieved by application of technical, legal, organizational, educational and other protective measures. To guarantee full security, it is necessary to ensure a mutual cohesion of individual components within the organization that operate simultaneously. If only one component is not safe, this deficiency cannot be effectively achieved and the system cannot be viewed as safe. For example, if the personnel policy is not implemented sufficiently as well as the related individual security, the human factor failure within the organization can overcome the costly security equipment, or perfectly mastered Occupational Safety and Health.

Today we need to look for innovative features in security technology, where the development is directed to implementing new access control systems, especially the whole spectrum of possibilities of biometric identification and verification. The areas of interest should also be the technologies for searching and profiling bad intentions of potential threats carriers, respectively an attack on protected interest. This concerns a development of contactless devices enabling to detect negative intention of a person towards his/her surroundings by sensors, meaning for example a potential terrorist entering the PU building. The system allows a registration of non-verbal body expressions, which cannot be seen by eye (e.g. body temperature, breathing rhythm, scanning contraction of facial muscles in real-time, analysis of body odor, etc.). If the system finds out that the sensed parameters are off the

normal condition, the alarming assessment follows and the operator can check the identified person in more details. The area of physical protection also starts applying a technology RFID. Its application has started in the faculties of Technical University of Ostrava, specifically the Faculty of Mining and Geology and the Faculty of Safety Engineering. The implementation of RFID technology allows the organization to obtain a contactless element of identification of persons and property, or their localization within the building in real time. Along with the optimal settings of regime measures, it forms an effective system allowing the control of input, output and movement of employees, students or visitors, with the possibility of their subsequent localization in public school facilities (Ščurek and Konečný, 2011).

Results

Identification and characteristics of RFID technology

RFID systems represent a modern contactless automatic identification system, operating on a principle of radio frequency. Using electromagnetic waves, the systems are able to facilitate the transfer of data, their recording, or to provide required information about objects in real time, so-called Real Time Locating System (RTLS). The RFID technology can be passive or active. Passive tags are appropriate for the identification of individuals. The active technology with RTLS does not primarily concern the identification of objects, but their localization and ability to emit, independently on the reader, a pre-defined signal with unique number. RTL systems are thus intended primarily for the monitoring of person's position in real time using an electronic device (active RFID transponder) located on desired object, which exchanges data with access points. The system is able to determine a position of specified individual within the PU area, based on the response and signal strength from at least three access points. The primary factor for functioning of the RTLS system in certain area is the availability of radio signal in particular, thus the existence of wireless infrastructure. With increasing frequency increases the transferability of data, but also decreases the quality of the RFID signal and the distance in which the reader is able to communicate with the tag. The optimal choice of frequency is the primary element in the implementation of the RFID system, which implies also a number of other restrictions, such as the sensor's range, speed of reading and recording, or the applicability of RFID technology itself (Finkenzeller, 2003).

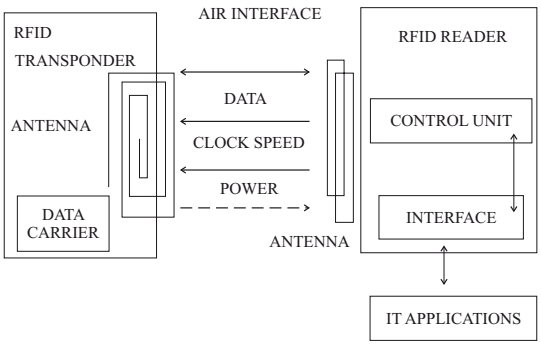

Fig. 1 Bloch diagram of RFID operation (Vojáček, 2008)

The sequence of the principle of operation of these systems is as follows:

- In the primary phase the reader emits an electromagnetic wave on its carrier frequency, that is accepted by the transponder antenna;
- Induced voltage causes an electric current which is rectified and feeds the capacitor in the transponder (accumulated energy is used for powering the logic circuits and radio transponder);
- When the capacitor voltage reaches the minimum required level, the logic automat or microprocessor are actuated (i.e. the control circuits within the transponder) and the transponder starts sending reply to the reader.

Transponder yielding provides a two-state modulation (Amplitude Shifting Key), which is realized by changing the terminating impedance of the transponder antenna (reflections generated by changing impedance of the antenna are detected by the reader and interpreted as logic levels 1 and 0). The quality of the RFID signal continuously declines with increasing distance between the reader and the transponder. Increase of noise in the primary signal leads to the impossibility of successful detection of the received message. The actual management of communication and states of communication chain are defined by relevant ISO standard (Finkenzeller, 2003). The fact that the tags are rewritable is important in terms of physical protection. The data stored on tags are transient and can be updated as needed. The specific object, on which the RFID tag is located, is then clearly identified by the EPC identification number, which is included together with other data in the memory chip of each tag and has a hierarchical structure (Vojtěch, 2011).

Application of RFID technology within the premises of Public universities

Point of interest in terms of physical protection is mainly to protect persons, property and other assets within the Public universities, which is closely related with the perimeter identification and monitoring the movement of persons inside individual PU's buildings. Given this fact, the next chapter focuses on personal and perimeter localization.

Localization of the perimeter, so-called Perimeter Locator, is an unconventional perimeter protection system, ensuring the monitoring and surveillance of the perimeter protection (fencing), using the special acceleration RFID tags that are installed on wire-netting fence and walk-through gates, which can detected potential intruders. Comprehensive system of this protection is contactless and the life-cycle of acceleration tags is several years. Perimeter Locator is optimal and easy to apply to protect the perimeter of public universities in terms of physical protection and in terms of their vulnerability. Perimeter localization system is able to communicate with all types of security system control panels, providing totally accurate guidance of CCTV cameras to the place of incident with an accuracy of 2 m. The principle of detecting intruders and undesirable effects is based on scanning of time and dynamic change in the position of the fence wire-netting, which is typical for overcoming the fence by potential intruder (Paleček, 2009).

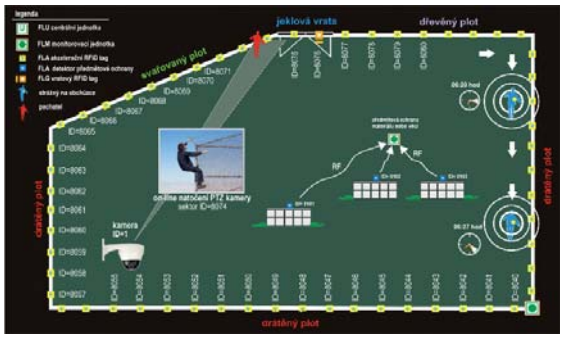

Fig. 2 Perimeter Locator System (Paleček, 2009)

The system is also able, through the parallel evaluation of the signal from each tag; to eliminate false alarms caused by for example adverse weather conditions, since such changes are induced on more than one RFID tag at a time. Perimeter Locator is also accurate in the detection of possible sabotage of the system. Sensors have a sophisticated algorithm of movement in three axes, allowing detecting any attempts of disassembly, sabotage or theft of the tags or parts of the fence, to which the tag is attached, even during the inactive mode. It is also an effective tool of physical protection in terms of perimeter protection, resulting in increasing security levels and protection of persons, property or other assets of public universities.

Another important element in the physical protection is the personal localization, the so-called Person Locator, representing an intelligent RTLS for monitoring the movement of people through personal active RFID tags in real time, in the 868 MHz frequency band. This frequency interface is dedicated only for RFID identification, thus it is possible to ensure, as opposed to the contention bands, the required accuracy of position detection of the monitored person. On the other hand, the disadvantage is just this single-purpose proprietary wireless infrastructure that is necessary to be built, maintained and used only for a single application - the RTLS, which is not quite optimal from the economic point of view. The system functioning on the above principle can be implemented for a identification of persons, monitoring employees, or for granting access and monitoring of specific groups of people in the buildings of public universities (Paleček, 2009). For this purpose, RTLS is being used effectively in building an Incubator of the Technical University of Ostrava, with the international RFID laboratory.

The personal localization system works independently of the behavior of monitored people and can also be used for getting information about the position and movement of all persons within the public university buildings. Precision of the monitoring of people in public universities buildings depends on the number of sensors that are installed at the door leading into the monitored zone. Due to this fact, the safety zones of each building can be precisely determined according to the level of authorization of people, and in case of unacceptable entry the system initiates the alarm signal. Therefore, it is also an intelligent security system that can be automatically put into the guarding mode after all monitored persons from different areas or rooms depart. Implementation of this active RFID technology represents a relatively high expense and we need to consider a speed of its return. Due to this fact it is necessary to perform an analysis of RFID technology installation, aimed at verifying the potential of implementation of this technology, accurately defining its benefits and characterizing possible safety and economic risks.

Should the organization require only the identification of individuals within the PU premises, it is possible to use for example ISIC cards or cards equipped with H4102 chip to identify people, since these cards are fully compatible with the reader. Practical example might be the lecture

halls, auditoriums, etc.; after finishing all activities (lectures, conferences, etc.) in those areas and leave of the last person the alarm system will get activated. In case of detection of potential disturbance, the system responds quite conventionally and reports alarm to required places, especially the centralized protection desk (Macůrek, 2005). For this purpose stationary and mobile RFID gates for entry and exit of vehicles may be established, but also turnstiles and modular RFID reader antennas can be applied, generating zones in entrances and doors.

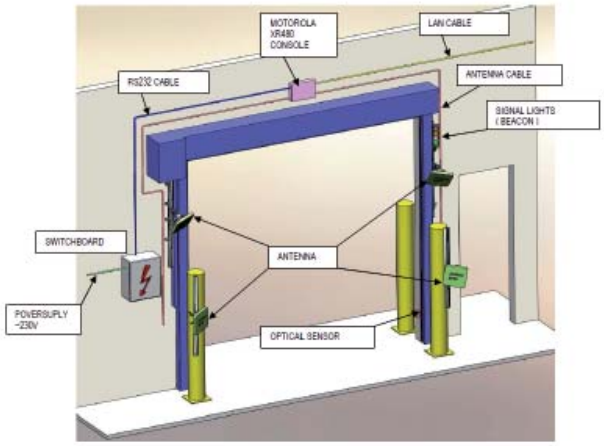

Fig. 3 Stationary RFID gate (Eprin, 2011)

The primary condition for effective implementation and management of these systems is to understand their functionality, but also risks resulting in their operation (Šenovský, 2008). Like other development systems, the RFID technology needs to be applied with a certain degree of foresight, taking into account various potential security risks. The primary weakness of RFID technology is a unique chip serial number, which is indelible and can be detected and potentially misused (Klonowski et al., 2008). The risk is also other information (e.g. personal) stored in the chip that are easily identifiable by mobile devices on the distance of several meters, due to the contactless operation of this technology. Among the important safety features eliminating the above risks are high-quality encryption using a symmetric encryption key, or at best the asymmetric cryptography technology. Another option of protection is creating secure communication channels based on predefined algorithms. These issues closely relate to the economic and operational exigency of these devices, including the capacity and performance limitations of RFID, where the chip can store only a limited number of strong encryption keys and algorithms, which is one of the main factors preventing the expansion of RFID technology in other areas of applicability and potential replacement of more preferred systems for identification and localization of persons, property or other assets of the organization. However, in the physical protection of public universities, this technology is adequate and effective in the elimination of security risks and represents an appropriate choice of the organization.

Safety risks related to the application of RFID technology

Just as other development technologies, the RFID systems have to be implemented with certain foresight and consideration of all consequent potential safety risks. The elementary weakness of RFID technology is the uniqueness of chip serial number, which is indelible and can be detected and possibly even misused. Other data (personal data) contained in the chip represent a threat as well, since they are easily identifiable by portable equipment within the distance of several meters due to the contact-free operating of this technology. Important security elements reducing the above risk include primarily a high-quality encryption using symmetric cipher key, or better the asymmetric cryptography (Mallahzadeh et al., 2012). Another manner of providing safety is an establishment of secure communication channel based on pre-defined algorithms. These issues closely relate to the financial and operational intensity of these devices, including RFID's capacity and performance restrictions enabling to save only a limited amount of strong ciphered keys and algorithms on the chip, which is one of the main factors preventing an expansion of RFID technology in other applicability areas and potential replacement of more preferred systems for identification and localization of individuals, property or other assets of the organization.

Conclusion

The article dealt with security threats and risks related to the physical protection of PU and their elimination using the potential implementation of RFID technology. We can expect fast future development of these systems in other applications of physical protection, including reduction of initial costs representing a primary aspect for implementation of RFID technology as an appropriate technical means increasing a level of particular building's security

References

EPRIN (2011). RFID - expediční brána [online] Eprin spol. s.r.o, Brno [cit. 2012-03-30]. Available at: http://www.eprin.cz/reseni/pripadove-studie/technologie-rfid/rfid-expedicni-brana# (in Czech).

FINKENZELLER, Klaus (2003): *RFID Handbook, second edition*. Germany 2003. 419 p. ISBN 0-470-84402-7.

KLONOWSKI, Marek, CICHOŃ, Jacek, & KUTYŁOWSKI, Mirosław (2008). Privacy protection for RFID with hidden subset identifiers [online]. Wroclaw: Institute of Mathematics and Computer Science, Wroclaw University of Technology, Poland, 2008 [cit. 2012-06-10]. Available at: http://www.scopus.com/record/display.url?eid=2-s2.0-44649174575&origin=resultslist&sort=plf-f&src=s&st1=Privacy+Protection+for+RFID+with+Hidden&sid=CVvON9ycsVwq_T9YDcw3kgX%3a580&sot=b&sdt=b&sl=54&s=TITLE-ABS-KEY%28Privacy+Protection+for+RFID+with+Hidden%29&relpos=3&relpos=3&searchTerm=TITLE-ABS-KEY(Privacy Protection for RFID with Hidden).

MACŮREK, Filip (2005). Radiofrekvenční identifikace RFID a její použití v automatizaci a logistice [online]. Automa, 2005, Vol. 11, No. 8-9. ISSN 1210-9592. Available at: http://www.odbornecasopisy.cz/index.php?id_document=30654 (in Czech).

MALLAHZADEH, Alireza, ALIAKBARI, Hanieh, NEZHAD, Sajad Mohammad Ali, (2012). A tri-band, small size radio frequency identification tag antenna with U-shaped slots, 2012 [online]. Microwave and Optical Technology Letters, 54(8), pp. 1975-1978. [cit. 2012-06-10]. Available at: http://www.scopus.com/record/display.url?eid=2-s2.0-84861351003&origin=resultslist&sort=plf-f&src=s&st1=+A+tri-band%2c+small+size+radio+frequency+identification+tag+antenna+with+U-shaped+slots&sid=CVvON9ycsVwq_T9YDcw3kgX%3a650&sot=q&sdt=b&sl=106&s=TITLE-ABS-KEY-AUTH%28+A+tri-band%2c+small+size+radio+frequency+identification+tag+antenna+with+U-shaped+slots%29&relpos=0&relpos=0&searchTerm=TITLE-ABS-KEY-AUTH(A tri-band, small size radio frequency identification tag antenna with U-shaped slots).

PALEČEK, Adam, (2009). RFID a RTLS technologie, [online]. Marsyas Development a.s. [cit. 2011-02-02]. Available at: http://www.7md.cz/reseni/perimetr-locator/ (in Czech).

ŘEHÁK, David, GIERTLOVÁ Zuzana (2011). Návrh ujednocení bezpečnostní termionologie fakulty bezpečnostního inženýrství VŠB - TU Ostrava. *Sborník vědeckých prací Vysoké školy báňské - Technické univerzity Ostrava, Řada bezpečnostní inženýrství.* Ostrava, 2011, Vol. VI, No. 2, pp. 63-66. ISSN 1801-1764 (in Czech).

ŠČUREK, Radomír, KONEČNÝ, Martin (2011). Aplikace analýzy rizik v oblasti fyzické ochrany veřejných vysokých škol. *Sborník vědeckých prací Vysoké školy báňské - Technické univerzity Ostrava, Řada bezpečnostní inženýrství*. Ostrava, 2011, Vol. VI, No. 1, pp. 27-32. ISSN 1801-1764 (in Czech).

ŠENOVSKÝ, Pavel (2008). Metody analýzy rizika prvků kritické infrastruktury. *SPEKTRUM*. 2008, Vol. 8, No. 1, pp. 40. ISSN 1211-6920 (in Czech).

VOJÁČEK, Antonín (2008). Více i méně běžné RFID frekvence a jejich vliv na komunikaci [online]. HW server s.r.o. [cit. 2012-03-26]. Available at: http://automatizace.hw.cz/vice-i-mene-bezne-rfid-frekvence-jejich-vliv-na-komunikaci (in Czech).

VOJTĚCH, Lukáš (2011). RFID - technologie pro internet věcí, [online]. Elektrotechnický magazín, ISSN 1803-6007 [cit. 2011-02-13]. Available at: http://pandatron.cz/?733&rfid_-_technologie_pro_internet_veci (in Czech).